CLAIMS

What is claimed is:

1. A copy protection method to prevent unauthorized copying of digital data during digital data transmission between a sender and a receiver, comprising:

encrypting a first region of a text containing a second encryption key using a first encryption key;

encrypting a second region of the text using the second encryption key; and

transmitting a cipher text comprising the encrypted first and second regions.

2. The copy protection method according to claim 1, further comprising:

transmitting the first encryption key, region segmentation information for segmenting the text into the first region and the second region, and information related to the second encryption key through a safe transmission path.

3. The copy protection method according to claim 1, wherein the first encryption key comprises an encryption key for use with a common key encryption method.

4. The copy protection method according to claim 1, wherein the first encryption key comprises a public key for use with a public key encryption method.

5. The copy protection method according to claim 1, wherein the second encryption key is smaller than the first encryption key where a common key encryption method is used.

6. The copy protection method according to claim 1, wherein a size of the first encryption key is fixed, and a size of the second encryption key is varied by a transmission unit within the first region.

7. The copy protection method according to claim 2, wherein the information related to the second encryption key includes size and position information of the second encryption key.

8. The copy protection method according to claim 7, wherein the position and size information of the second encryption key are fixed.

9. The copy protection method according to claim 7, wherein the position and size information of the second encryption key are varied.

10. The copy protection method according to claim 2, wherein the first region of the text is smaller than the second region of the text.

11. The copy protection method according to claim 2, wherein the region segmentation information comprises information on a starting address of the second region of the text.

12. The copy protection method according to claim 2, further comprising:

decrypting the first region of the transmitted cipher text using the transmitted first encryption key and the transmitted region segmentation information;

extracting the second encryption key from the decrypted first region using the transmitted information related to the second encryption key; and

decrypting the second region of the transmitted cipher text using the extracted second encryption key.

13. A copy protection method for decrypting a cipher text received from a sender who encrypts a first region of a text containing a second encryption key information using a first encryption key, encrypts a second region of the text using the second

encryption key based upon the second encryption key information, and transmits the cipher text, the first encryption key, region segmentation information, and second encryption key information to a receiver, comprising:

decrypting the first region of the cipher text using the transmitted first encryption key and the transmitted region segmentation information;

extracting the second encryption key from the decrypted first region using the transmitted second encryption key information; and

decrypting the second region of the cipher text using the extracted second encryption key.

14. The copy protection method according to claim 13, wherein a size of the first encryption key is fixed, and a size of the second encryption key is varied according to a transmission unit within the first region.

15. The copy protection method according to claim 13, wherein the first region of the text is smaller than the second region of the text, and a size of the first encryption key is larger than a size of the second encryption key.

16. The copy protection method according to claim 2, wherein the region segmentation information comprises information on a size of the first region of the text.

17. The copy protection method according to claim 3, wherein the large first encryption key comprises an encryption key that is 56 bits or more.

18. A computer readable medium encoded with processing instructions for implementing a method of encrypting a text sent between a sender and a receiver performed by a computer, the method comprising:

encrypting a first region of the text using a first encryption key, where the first region contains a second encryption key; and

encrypting a second region of the text using the second encryption key.

19. The computer readable medium according to claim 18, further comprising sending the first encryption key and information related to the second encryption key through a safe transmission path.

20. The computer readable medium according to claim 19, wherein the first encryption key comprises a symmetric key having 56 bits or more.

21. The computer readable medium according to claim 19, wherein the first encryption key comprises an asymmetric key for use with an asymmetric key encryption method.

22. The computer readable medium according to claim 18, wherein the second encryption key is smaller than the first encryption key.

23. The computer readable medium according to claim 18, wherein a size of the first encryption key is fixed, and a size of the second encryption key is varied by a transmission unit within the first region.

24. The computer readable medium according to claim 19, wherein the information related to the second encryption key includes size and position information of the second encryption key.

25. The computer readable medium according to claim 24, wherein the position and size information of the second encryption key are fixed.

26. The computer readable medium according to claim 24, wherein the position and size information of the second encryption key are varied.

27. The computer readable medium according to claim 19, wherein the first region is smaller than the second region.

28. The computer readable medium according to claim 24, further comprising sending information on a starting address of the second region through the safe transmission path.

29. The computer readable medium according to claim 28, further comprising

sending a cipher text comprising the encrypted first and second portions through an unsafe transmission path; and

obtaining the safe transmission path through authentication operations.

30. A computer readable medium encoded with processing instructions for implementing a method of decrypting an encrypted text sent between a sender and a receiver performed by a computer, the method comprising:

decrypting a first region of the encrypted text using a first encryption key, where the first region contains a second encryption key;

decrypting a second region of the encrypted text using the second encryption key.

31. The computer readable medium according to claim 30, wherein said decrypting the first region further comprises:

decrypting the first region using region segmentation information; and

extracting the second encryption key from the decrypted first region using information related to the second encryption key.

32. The computer readable medium according to claim 31, wherein the region segmentation information, the information related to the second key, and the first encryption key are received through a safe transmission path.

33. The computer readable medium according to claim 32, further comprising receiving the encrypted text through an unsafe transmission path.

34. The computer readable medium according to claim 30, wherein a size of the first encryption key is fixed, and a size of the second encryption key is varied according to a transmission unit within the first region.

35. The computer readable medium according to claim 30, wherein the first region of the text is smaller than the second region of the text, and a size of the first encryption key is larger than a size of the second encryption key.

36. A sender for sending encrypted text, comprising:

an authenticator to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are sent; and

an encryptor to encrypt a text using the first encryption key and the second encryption key, where the second encryption key is extracted from a portion of the text encrypted by the first encryption key.

37. The sender of claim 36, wherein

the information related to the second encryption key comprises size and position information of the second encryption key, and

the encrypted text is sent through an unsafe transmission path.

38. The sender of claim 37, wherein the sender comprises an information appliance.

39. The sender of claim 37, wherein the sender comprises a computer.

40. The sender of claim 37, wherein the sender comprises a server.

41. A receiver for receiving encrypted text, comprising:

an authenticator to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are received, and

a decryptor to decrypt a portion of the text using the first encryption key, to extract the second encryption key from the decrypted portion using the information related to the second encryption key, and to decrypt another portion of the text using the second encryption key.

42. The receiver of claim 41, wherein

the information related to the second encryption key comprises size and position information of the second encryption key, and

the encrypted text is received through an unsafe transmission path.

43. The receiver of claim 42, wherein the sender comprises an information appliance.

44. The receiver of claim 42, wherein the sender comprises a computer.

45. The receiver of claim 42, wherein the sender comprises a server.